InsideCounsel
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
December 13, 2013

Opinion

Technology: Auto-delete and the not-so-safe harbor

The safe harbor for ESI has not provided reliable shelter from sanctions storms

By Gareth Evans and Lauren Eber

At no time is the burden of a legal hold more acute than when a company determines that it must suspend auto-delete on an information system. And the "safe harbor" for electronically stored information (ESI) lost as a result of the routine, good faith operation of an information system often does not provide much protection.

The regular purging of electronic data is a necessary feature of many such systems. Indeed, databases containing sales information, payroll records, billing records, customer service call logs and all manner of other information rely upon auto-delete and overwriting to function.

When potentially relevant information resides on systems with automated purging, companies face a Hobson's choice in implementing a legal hold. If a company suspends the purging, it faces the prospect of keeping vast quantities of electronically stored information, with no assurance that the ESI will ever, in fact, be needed in the litigation. Suspending auto-delete can be prohibitively burdensome and expensive. It can even render some systems inoperable, as they may have limitations on the number of records they can maintain. If the company allows the automatic deletion, however, it risks potentially devastating spoliation sanctions.

And the safe harbor? Unfortunately, it has not provided reliable shelter from sanctions storms, at least when it comes to suspending auto-delete. Adopted as part of the 2006 e-discovery amendments to the Federal Rules of Civil Procedure, the Rule 37(e) safe harbor provides that, "absent exceptional circumstances," a court may not impose sanctions under the Federal Rules for ESI "lost as a result of the routine, good-faith operation of an electronic information system."

Although Rule 37(e) is at the center of another round of proposed amendments to the Federal Rules to deal with problems related to e-discovery — such as over-preservation, the lack of uniform national standards, and the imposition of sanctions based on negligence — any revisions are not likely to be implemented for at least a year, and it is unclear whether they will provide any greater protection with respect to automatic purging than the current rule.

Current Rule 37(e) itself was intended to tackle the problem of over-preservation and to address the fact that it can be difficult — and even impossible — to interrupt the routine operation of computer systems to preserve information that they overwrite, update or delete on an ongoing basis. It also recognized that it would be unfair to infer an intent to destroy evidence from the inadvertent loss of such ESI. Rule 37(e) was therefore intended to preclude sanctions based on negligence in such circumstances.

It hasn't exactly worked out that way, as more than a few courts arguably have not applied the rule as intended, a fact that should sound a note of caution regarding the current proposed rule amendments, which have similar goals. Some courts have held, for example, that Rule 37(e) does not apply once a duty to preserve has arisen. But that is arguably exactly when the rule is supposed to apply, provided that the responding party acted in good faith. Otherwise the rule would be unnecessary.

Although the Civil Rules Advisory Committee intended the phrase "absent exceptional circumstances" to apply where the requesting party is seriously prejudiced from the loss of relevant information, some courts have found the failure to suspend auto delete itself to constitute an "exceptional circumstance." Perhaps anticipating such an outcome, former chair of the Advisory Committee, Judge Lee H. Rosenthal, presciently rejected the "safe harbor" label for Rule 37(e), saying, "Anything that starts with the words 'absent exceptional circumstances' is not a safe harbor."

Some courts have also arguably misapplied Rule 37(e)'s good faith standard, which was intended to withhold protection only where parties act intentionally or recklessly in allowing relevant information to be lost or destroyed. These courts have instead sanctioned parties that took affirmative, though ultimately inadequate, steps to preserve the information.

Granted, Rule 37(e) was never designed to provide protection where a party consciously fails to suspend auto-delete with the intent of depriving the requesting party of relevant information. The Advisory Committee Note states that the good faith requirement means that a party cannot "exploit" the routine operation of an information system to "thwart discovery obligations." One in-house lawyer pointedly testified in the public hearings regarding the rule, "I think it would be insanity beyond belief for anybody, any serious lawyer, to advise their client that, oh, yeah, this is a way to get rid of something that might come back to bite us."

Courts will also be disinclined to apply the safe harbor where a party acts with deliberate ignorance — the "clear heart, empty head" scenario. Companies and their counsel should consider the potential sources of relevant information, whether those systems have auto-delete functions, and how they may preserve potentially relevant information on those systems. That does not mean that all information in a database necessarily must be placed under a legal hold. The duty to preserve applies to relevant information, not all information, in the database.

What are a company's options upon determining it should preserve information residing on a system with auto-delete? If it is not possible or practicable to suspend automated purging, and the relevant information is limited — i.e., not the entire database or a large portion of it — it may make sense to export the relevant records and save them to a more permanent storage medium, rather than preserving them in place. If the entire database or a large portion of it must be preserved, options include exporting all the records to another medium, creating a special backup, or retaining certain backup tapes.

Each option has its costs and benefits. Relying upon backup tapes for preservation, for example, can lead to substantial downstream costs when the information must be restored and the database recreated. Deciding which approach to take, and actually implementing it, should be accomplished with the assistance of counsel and technical personnel with the appropriate expertise to ensure that it is done in a defensible fashion. Without a reliable safe harbor, companies need an expert captain and crew to get them safely through the storm. ■

About the Authors

Gareth Evans

Gareth Evans is a partner at Gibson Dunn. His practice focuses on complex litigation, including information technology, data privacy and e-discovery.

Lauren Eber

Lauren Eber is an associate at Gibson Dunn. Her practice focuses on complex litigation, including information technology, data privacy and e-discovery.